

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA, : CRIMINAL NO.
:
v. :
:
NICHOLAS STENGEL, :
Defendant. :

FILED
JUL 17 2018
Clerk, U.S. District and
Bankruptcy Courts

STATEMENT OF OFFENSE

The parties in this case, the United States of America and the defendant, Nicholas Stengel, stipulate and agree that the following facts are true and accurate. These facts do not constitute all of the facts known to the parties concerning the charged offense; they are being submitted to demonstrate that sufficient facts exist that the defendant committed the offenses to which he is pleading guilty: Receipt of Child Pornography, in violation of 18 U.S.C. § 2252A(a)(2), and Laundering of Monetary Instruments, in violation of 1956(a)(2)(A).

Statement of Facts

A. The Website

Beginning in September 2017, law enforcement initiated a large scale investigation into a Tor based child pornography website, hereinafter referred to as “The Website.”¹ Tor is a computer network designed to facilitate anonymous communication over the Internet. The Tor

¹ The actual name of “The Website” is known to law enforcement. The disclosure of the name of The Website would potentially alert its users to the fact that law enforcement action is being taken against users of The Website, thereby provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, to protect the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the website will be identified herein as “The Website.”

network does this by routing a user's communications through a globally distributed network of relay computers, or proxies, rendering conventional Internet Protocol ("IP") address-based methods of identifying users ineffective. To access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle." When a Tor user accesses a website, only the IP address of the last relay computer (the "exit node"), as opposed to the user's actual IP address, appears on the website's IP address log. Currently, there is no practical method to trace a user's actual IP address back through those Tor relay computers. The Tor Network also makes it possible for users to operate websites, called "hidden services," in a manner that conceals the true IP address of the computer hosting the website.

The Website operated as a hidden service on the Tor network until March of 2018. The Website was used to host and distribute video files depicting child pornography that could be downloaded by site users. In fact, the upload page on The Website clearly states: "Do not upload adult porn." Any user could create a free account on The Website by creating a username and password. Only after the user registered an account could the user browse previews of videos available for download and post text to The Website. To download videos from the site, users must use "points," which are allocated to users by The Website. A registered user could earn points from The Website in several ways: (1) uploading videos depicting the sexual exploitation of children; (2) referring new users to The Website; (3) paying for a "VIP" account, which lasted for six months, entitled a user to unlimited downloads, and was priced at 0.03 Bitcoin (approximately \$327.60 USD as of March 1, 2018); or (4) paying for points incrementally.²

² Bitcoin ("BTC") is a type of virtual currency, circulated over the internet. BTC are not issued by any government, bank, or company, but rather are controlled through computer software operating via a decentralized, peer-to-peer network. BTC is just one of many varieties

As of February 8, 2018, The Website had over 125,000 unique videos available for downloading. In order to prevent duplicate videos from being uploaded, The Website provided a digital hash-value check in order for the user to compare his or her video to other videos previously uploaded to the site. The Website did not allow a user to upload a video whose hash value matched something previously uploaded to the site. According to law enforcement's viewing of The Website as of February 8, 2018, the videos stored on The Website amounted to over seven terabytes of data. As of February 8, 2018, The Website indicated on its download page details that its users had downloaded files from The Website more than one million times.

B. Defendant's Laundering of BTC to Promote Specified Unlawful Activity

Law enforcement identified the defendant's BTC account number, created on October 21, 2016, as having made at least 10 payments to The Website. Notably, between October 24, 2016 and July 13, 2017, the defendant transmitted 0.3801 BTC, worth approximately \$376.97, over at least six transactions to The Website. For example, on or about October 24, 2016, the defendant transmitted 0.1305 BTC from a location in Washington, D.C. to a BTC wallet associated with The Website, which was in South Korea.

Law enforcement's review of the forensic image of the electronic storage devices that had hosted The Website revealed that between April 4, 2017 and October 6, 2017 (186 day

of virtual currency. To acquire BTC, a typical user purchases them from a BTC virtual currency exchange. A virtual currency exchange is a business that allows customers to trade virtual currencies for other forms of value, such as conventional fiat money (e.g., U.S. dollars, Russian rubles, euros). Exchanges can be brick-and-mortar businesses (exchanging traditional payment methods and virtual currencies) or online businesses (exchanging electronically transferred money and virtual currencies). Virtual currency exchanges doing business in the United States are regulated under the Bank Secrecy Act and must collect identifying information about their customers and verify their clients' identities. It was through this "know your customer" policy that law enforcement were able to identify the defendant's BTC account number associated with payments to The Website.

sample), the defendant's username on The Website, PANZA73, downloaded 2,686 videos from The Website. Examples of the video descriptions downloaded from The Website include, "9y babe geting fuck in the pussy," "2 Girls 9yo masturbation," "Girl 10yo fun and the end suck dad," "5yo playing her vagina with her mom licking and masturbating," and "13 year old small girl takes a makeup brush both in ass and pussy." The combined length of time for the videos downloaded by the defendant from The Website during this limited time-frame is approximately 455,018.53 hours and consists of 163,909,873,126 bytes of data.

C. Defendant's Electronic Devices

On March 15, 2018, law enforcement applied for a search warrant to search the defendant's residence and place of employment in Washington, D.C., and to forensically analyze digital devices seized as a result of the information learned from the The Website's servers.

On March 22, 2018 at approximately 6:05 am, law enforcement executed the search warrant at the defendant's residence located in Washington, D.C. Law enforcement announced "police" and "warrant" while at the defendant's front door. After a short period of time, the defendant's wife complied with law enforcement's requests and opened the door. Law enforcement called for the defendant to appear, and reiterated "police" and "warrant," however the defendant failed to comply with the requests. Law enforcement proceeded through the residence in order to locate the defendant, who was subsequently located in the bathroom, standing in the bathtub, holding a knife. The defendant was ordered to drop the knife and he complied. Law enforcement immediately observed that the defendant had multiple deep lacerations to both of his wrists and his neck and observed that he had lost a lot of blood. The defendant was assisted out into the living room so he could receive immediate medical aid.

As law enforcement was treating the defendant's wounds, he spontaneously stated "for your search, look there and there," while pointing to a laptop and a messenger bag in the living room. Law enforcement clarified that the defendant was pointing to the Asus laptop and messenger bag, and he replied yes. The defendant was subsequently transported to George Washington Hospital for life-saving medical treatment.

At the defendant's residence, law enforcement seized an Asus laptop with S/N/FBN0CJ04807146g, a Toshiba hard-drive with serial number 25LBTIZVTPDC, a Western Digital hard-drive with S/N WCAZA0085789T, and a Quantum Fireball 20.4 gigabyte hard-drive with S/N 041RRT-12545-0C4-15WN, Nexus Tablet with S/N K008DAOKBC118683, and Acer Laptop with S/N LXRMU0209513236D0A1601, among other items. While on site, a Computer Forensic Analyst (CFA) with HSI performed a preliminary forensic preview of some of the electronic devices. The CFA identified child pornography files on the Asus laptop, the Toshiba hard-drive, and the Quantum Fireball 20.4 gigabyte hard-drive. The Toshiba hard-drive was located in the messenger bag that the defendant had identified as belonging to him to law enforcement. The defendant's wife also identified that this messenger bag belonged to the defendant.

Law enforcement subsequently performed a more in-depth forensic analysis of the Asus laptop and Toshiba hard-drive. Located on both the Toshiba hard-drive and Asus laptop were links to the defendant's username on The Website of "PANZA73." Law enforcement identified more than 6,000 videos and 600,000 images depicting child pornography located on the Toshiba hard-drive. An example of the depictions located on the hard-drive includes a file folder entitled "YFCU" containing a series of images of a child, who appears approximately five years old, laying on a bed with her vagina exposed and the final image depicting the same child's vagina

being penetrated by an adult penis. Law enforcement identified more than 100 videos and 5,000 images depicting child pornography on the Asus laptop. In addition, law enforcement identified on the Asus laptop the TOR software, which is used to access The Website. Examples of videos and images located on the Asus laptop include the following:

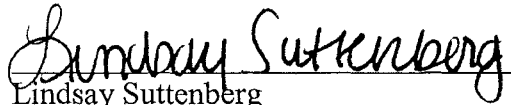
- A video titled IMG_0199 mov: This video shows a pre-pubescent girl, naked from the waist down and laying on a bed in what appears to be a young girl's bedroom based on the décor of the room. Her legs are spread apart and she is inserting an object into her anus and rubbing it against her vagina. Thereafter, she inserts the object into her mouth. This video was produced by an individual, located in Texas, of his (approximately) 9-year-old adoptive daughter. This individual uploaded this video to several Tor websites, including The Website. Law enforcement identified the individual who produced and uploaded this video, and he admitted to producing these videos of his daughter and uploading them to various sites, including The Website.
- Image titled X_3BCA3408.JPEG: This image depicts a girl, approximately 8 years old, with her legs bound by rope at the ankles and spread over her head with her vaginal area exposed and the focal point of the depiction.
- A video titled 2018_02-22-13-50-44 mp4: This video depicts a child, approximately 3-4 years old, laying naked on a bed and touching her exposed vagina.
- A video titled "Al&boy.mp4:" This video shows a prepubescent male child, approximately eight years old, and a prepubescent female child, approximately six years old, engaged in sexual activities with each other. The female child is seen performing fellatio on the male child and the male child is seen engaging in vaginal intercourse with the female child.
- A video titled "beavs-girl-05.mp4:" The video shows a prepubescent female child, approximately five years old, sitting on a bed with her legs spread and her vagina exposed and the focal point of the depiction. An adult male is seen masturbating and subsequently ejaculating onto the child's vagina.

D. Defendant's Prior Conviction

On February 24, 2003, the defendant pled guilty in the United States District Court for the District of Columbia for violations of 18 U.S.C. §§ 2252A(a)(2) and 2256(8)(A) (Certain Activities Relating to Material Constituting or Containing Child Pornography).

Respectfully submitted,

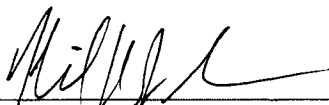
JESSIE K. LIU
UNITED STATES ATTORNEY


Lindsay Suttenger
Zia Faruqui
Youli Lee
Assistant United States Attorneys

DEFENDANT'S ACKNOWLEDGMENT

I have read every page of this Statement of the Offense and have discussed it with my attorney. I fully understand this Statement of the Offense. I agree and acknowledge by my signature that this Statement of the Offense is true and accurate. I do this voluntarily and of my own free will. No threats have been made to me nor am I under the influence of anything that could impede my ability to understand this Statement of the Offense fully.

Date: 7/17/18




Nicholas Stengel
Defendant

ATTORNEY'S ACKNOWLEDGMENT

I have read every page of this Statement of the Offense, and have reviewed it with my client fully. I concur in my client's desire to adopt this Statement of the Offense as true and accurate.

Date: 7-17-18



Allen Dale
Defense Counsel